YRITYKSEN TIETOVERKON UUDISTAMINEN

Runtech Systems Oy

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Opinnäytetyö
Kevät 2011
Jarno Kurlin

Lahden ammattikorkeakoulu
Koulutusohjelma

KURLIN, JARNO: Yrityksen tietoverkon uudistaminen

Tietoliikennetekniikan opinnäytetyö, 67 sivua, 14 liitesivua

Kevät 2011

TIIVISTELMÄ

Tämän opinnäytetyön aiheena on yrityksen tietoverkon uudistaminen. Työn tavoitteena on suunnitella ja toteuttaa toimiva ja hyvin dokumentoitu tietoverkkoratkaisu Runtech Systems Oy:lle. Toimiva ja helposti laajennettavissa oleva tietoverkko luo hyvät edellytykset yrityksen toimintaa helpottavien palveluiden asentamiselle ja ylläpitämiselle.

Lähiverkkojen tekniikan osalta tutustutaan lähiverkon kaapelointiin, aktiivilaitteisiin sekä vikasietoisen lähiverkon suunnitteluun ja teteutukseen. Nykyisin lähiverkkojen kaapelointi toteutetaan lähes poikkeuksetta yleiskaapelointijärjestelmän mukaisesti. Lähiverkon aktiivilaitteet ovat tietoliikennepaketteja ohjaavia laitteita, joiden avulla paketteja kuljetetaan lähiverkossa mahdollisimman nopeasti laitteelta toiselle. Yleisimpiä lähiverkon aktiivilaitteita ovat kytkimet, ja osittain myös reitittimet, jotka välittävät tietoliikennepaketteja eri virtuaaliverkkojen välillä.

Yrityksen lähiverkot voidaan yhdistää useilla erilaisilla VPN-ratkaisuilla, jotka eroavat toisistaan lähinnä toteutuksen hinnan ja helppokäyttöisyyden suhteen. Lähiverkkojen yhdistäminen voidaan tehdä Internetin välityksellä, tai jättää yhdistäminen tietoliikenneoperaattorin vastuulle, jolloin operaattori yhdistää lähiverkot operaattoriverkon ylitse esimerkiksi MPLS-tekniikan avulla.

Mikäli lähiverkot yhdistetään itse, jää ratkaisuksi joko VPN-ominaisuuksia sisältävien palomuurilaitteiden asentaminen molempiin lähiverkkoihin tai lähiverkkojen yhdistäminen ohjelmallisen VPN-ratkaisun avulla. Ohjelmalliset VPN-ratkaisut jakautuvat kaupallisiin ja vapaan lähdekoodin ohjelmistoihin. Yksi suosituimmista ilmaisesta ohjelmista on OpenVPN, jonka avulla voidaan yhdistää keskenään joko kaksi lähiverkkoa, tai lähiverkko ja yksittäinen käyttäjä.

Resurssien salliessa yrityksen palvelimet kannattaa asentaa virtuaalipalvelimille, jolloin uuden palvelimen käyttöönotto on nopeaa ja kustannustehokasta. Lähiverkon toiminnan kannalta tärkeimpiä palvelimia ovat erilaiset osoite- ja nimipalvelimet. Yrityksen toiminnan kannalta tärkeimpiä palvelimia ovat tulostus, tieto- ja hakemistopalvelimet.

Tietoverkon dokumentointi on ylläpitäjän tärkein työkalu siinä vaiheessa, kun tietoverkossa ilmenee jotain vikaa. Dokumentaation tekemiseen saattaa kulua aikaa, mutta hyvin tehtynä dokumentaatio nopeuttaa vian selviämistä ja näin ollen saattaa tuoda suuria säästöjä yritykselle.

Avainsanat: Lähiverkkojen tekniikka, VPN-ratkaisut, virtuaalipalvelimet, tietoverkon dokumentointi

Lahti University of Applied Sciences
Degree Programme in Information Technology

KURLIN, JARNO: Improving the information network of a company

Bachelor's Thesis in Telecommunications Technology, 67 pages, 14 appendices

Spring 2011

ABSTRACT

This Bachelor's thesis is about improving the information network of a company. The main goal was to plan and implement a well-documented information network for Runtech Systems Ltd. A functional and easily expandable network creates a good basis for the system administrator to install and maintain the company's essential information services.

The section of the thesis dealing with local area network technology describes cabling standards, active network devices and instructions for how to plan and implement a redundant local area network. Local area network devices forward information packets through a network as quickly as possible. The most common active network device is a switch. Routers are also well-known active devices in a network, but in fact routers are not classified as local area network devices.

Corporate local area networks can be connected in different ways, which differ mostly in price and usability. Local area networks can be connected via Internet or the connection can be left entirely to the service provider's responsibility. The service provider usually connects local area networks through their core network with MPLS technology.

If local area networks are connected via Internet, the two most common solutions are to install firewall devices to both ends, or to connect networks with a software based VPN solution. Software based VPN solutions are divided into commercial and open source software. One of the most popular open source VPN solutions is OpenVPN which can be used to connect local area networks. OpenVPN also allows individual users to connect to a corporate network from the Internet.

Server virtualization is a good way to speed up a company's server installation and to decrease server maintaining expenses. The most important servers for network operability are address servers and name servers. On the other hand, the most important servers for the company's employees are printing servers, information servers and file servers.

Well-planned documentation is the best tool for the administrator when an information network is not working as it is supposed to. Implementing good documentation can take a great deal of a time, but when it is finished, it accelerates problem solving and thereby brings huge savings by decreasing the downtime of the network.

Key words: local area networks, VPN solutions, server virtualization, documentation of the information network

SISÄLLYS

Lyhenneluettelo

AH	Authentication header, todennusotsikko.
BIND	Berkeley Internet Name Domain, turvallisuuskuorman enkapselointi.
BPDU	Bridge procotol data unit, siltaprotokollan tietoyksikkkö.
CentOS	Community ENTerprice OS.
DDR3	Dual data rate 3, kaksoisdatavauhti 3.
DHCP	Dynamic host configuration protocol, dynaaminen isäntäasetusprotokolla.
DN	Distinguished Name, piilotettu nimi.
DNS	Domain name system, nimipalvelujärjestelmä.
ESP	Encapsulating security payload, turvallisuuskuorman enkapsulointi.
FTP	File transfer protocol, tiedonsiirtoprotokolla.
GRE	Generic routing protocol, yleinen reititysprotokolla.
HTTPS	Hypertext Transfer Protocol Secure, turvattu hypertekstinsiirtoprotokolla,
ICMP	Internet control message protocol, Internet ohjausviestiprotokolla.
IGMP	Internet group management protocol, Interenet ryhmähallintaprotokolla.
IIS	Internet Information Services, Internet tietopalvelut.
IKE	Internet key exchange, Internet avainvaihto.
IP	Internet protocol, Internetprotokolla.
IPsec	Internet protocol security, Internet protokollan turvallisuus.
L2F	Layer 2 forwarding, tason 2 uudelleenohjaus.
L2TP	Layer 2 tunnel protocol, tason 2 tunnelointiprotokolla.
LDAP	Lightweight Directory Access Protocol, kevyt hakemistoselausprotokolla.
MAC	Media Access Control, Mediapääsyn hallinta.
MD5	Message digest 5, viestitiivistelmä 5.
MPLS	Multiprotocol label switching, moniprotokolla lipukekytkentä.
MPPE	Microsoft Point-to-Point Encryption, Microsoftin pisteestä pisteeseen salaus.
MSTP	Multiple Spanning Tree Protocol, usean puuvirityksen protokolla.
NAT	Network address translation, verkko-osoitteen muunnos.
NetBIOS	Network basic input/output system, verkon perus sisään/ulos järjestelmä.

OSI	Open Systems Interconnection, avointen järjestelmien yhteys.
PEM	Privacy Enhanced Mail, yksityisyysparanneltu posti.
PKCS#12	Public-key cryptography standards #12, julkisen avaimen salausstandardit #12
POP3	Post office protocol 3, postitoimistoprotokolla 3.
PPP	Point-to-Point protocol, pisteestä pisteeseen protokolla.
PPTP	Point to Point Tunneling Protocol, pisteestä pisteeseen tunnelointiprotokolla.
RADIUS	Remote authentication dial in user service, käyttäjien etätodennussisäänsoittopalvelu.
RFC	Request for comments, kommenttien pyyntö.
RSTP	Rapid Spanning Tree Protocol, nopea virityspuuprotokolla.
SATA	Serial Advanced Technology Attachment, sarja kehittynyt teknologialiite.
SIP	Session initiation protocol, istunnonaloitusprotokolla.
SMTP	Simple mail transfer protocol, yksinkertainen postinsiirtoprotokolla.
SSH	Secure shell, turvallinen komentokehote.
SSL VPN	Secure socket layer virtual private network, turvallisuuskahvakerroksen virtuaalinen yksityisverkko.
TCP	Transmission control protocol, siirronhallintaprotokolla.
TCP/IP	Transmission control protocol/Internet procotol, siirronhallintaprotokolla/internet protokolla.
TLS	Transport layer security, siirtokerroksen turvallisuus.
UDP	User datagram protocol, käyttäjän datagrammiprotokolla.
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko.
VPN	Virtual Private Network, virtuaalinen yksityisverkko.
VTUN	Virtual tunnel, virtuaalinen tunneli.
WINS	Windows Internet Name Services, Windows Internetnimipalvelut.
WLAN	Wireless local area network, langaton lähiverkko.
WWW	World wide web, maailmanlaajuinen verkko.
WebDAV	Web-based Distributed Authoring and Versioning, web-pohjainen jaettu sisällöntuotanto ja versiointi.

1 JOHDANTO

Nykyaikaisen yritystietoverkon rakentamiseen vaaditaan useita verkon aktiivilaitteita sekä palvelimia. VPN-ratkaisujen (Virtual Private Network) avulla yrityksen toimipisteet saadaan yhdistettyä siten, että useat yksittäiset lähiverkot saadaan yhdistettyä toisiinsa, ja niissä toimivat palvelut voidaan jakaa kaikkien verkon käyttäjien kesken. Monissa toimipisteissä toimiville palveluille asetetaan usein korkeat toimintavaatimukset, ja käyttäjien tulee olla tyytyväisiä käyttämiensä palveluiden tasoon. Näiden vaatimusten täyttämiseen vaaditaan verkon suunnittelijoilta paljon, ja useimmiten yritykset ulkoistavatkin kyseiset toiminnot niihin erikoistuneille yrityksille.

Tämän työn tarkoituksena on tutustua yrityksen tietoverkon suunnitteluun ja toteutukseen. Teoriaosuudessa työ perehdyttää lukijan lähiverkkoihin, lähiverkkojen VPN-ratkaisuihin, tietoverkon palveluihin sekä tietoverkon dokumentointiin. Lähiverkko-osuudessa käydään lävitse lähiverkon aktiivilaitteita, kaapelointia ja vikasietoisen lähiverkon toteutusta. Etäyhteysosiossa tutkitaan etäyhteyksien tekniikkaa, yhdistamistekniikoita, yhteysmuotoja sekä tunnelointitapoja. Palvelinosiossa tutustutetaan lukija yleisimpiin yrityksen tarvitsemiin palveluihin, ja lähiverkon dokumentoinnissa tutustutetaan lukija hyvän tavan mukaiseen tietoverkon dokumentointiin.

Tämän työn tavoitteena on löytää PK-yritykselle parhaat mahdolliset lähiverkon aktiivilaitteet, VPN-ratkaisut sekä tietoverkon palvelut. Tavoitteena on myös käyttää mahdollisimman paljon avoimen lähdekoodin alaisia palveluita, jolloin lisenssimaksujen osuus tietoverkon kustannuksissa saadaan alhaiseksi.

Käytännön osuudessa päivitetään yrityksen lähiverkon aktiivilaitteet uudempiin, yhdistetään yrityksen kaksi toimipistettä VPN-tekniikalla sekä asennetaan tietoverkkoon yrityksen tarvitsemat palvelut käyttäen hyväksi palvelinvirtualisointia. Koska työn tarkoituksena on toteuttaa yritykselle turvallinen tietoverkko, käytännön osuutta ei julkaista julkisesti.

2 LÄHIVERKKO

2.1 Lähiverkon aktiivilaitteet

Lähiverkon aktiivilaitteet ovat tietoliikennepaketteja ohjaavia laitteita, joiden avulla paketit kuljetetaan pisteestä pisteeseen lähiverkossa. Lähiverkon aktiivilaitteita ovat muun muassa toistimet, keskittimet, sillat, kytkimet sekä osittain myös reitittimet. (Keogh 2001, 99 – 107.)

Toistin on OSI-mallin (Open systems interconnection) fyysisellä kerroksella toimiva laite, jonka avulla ehkäistään signaalien vaimentumista lähiverkoissa. Toistin kytketään kahden kaapelin väliin, jolloin toistimen toimintaperiaatteesta riippuen toistin joko uudelleenmuodostaa signaalin kokonaan uudestaan, tai vain vahvistaa signaalia, ja lähettää signaalin edelleen eteenpäin. Uudelleenmuodostamisen avulla saadaan aikaiseksi selkeämpi signaali kuin pelkällä signaalin vahvistamisella. (Keogh 2001, 100 – 101.)

Keskittimien avulla voidaan kytkeä verkon päätelaitteet, esimerkiksi tietokoneet itse verkkosegmenttiin. Keskittimet voivat olla passiivia, aktiivisia tai älykkäitä. Passiiviset keskittimet kytkevät vain kaapelien päät yhteen, eivätkä muodosta signaaleita uudelleen. Aktiiviset keskittimet taas kytkevät kaapelien päät yhteen, sekä uudelleenmuodostavat signaalit aina ennen lähettämistä. Älykkäät keskittimet osaavat toimia myös kytkiminä, jolloin niiden avulla voidaan vähentää verkkoliikennettä lähiverkossa. (Keogh 2001, 102 – 103.)

Sillat ovat OSI-mallin datalinkkikerroksella toimivia laitteita, joiden avulla voidaan kytkeä yhteen useita verkkosegmenttejä. Silta kytketään kahden lähiverkon väliin siten, että silloilla todellisuudessa on fyysinen osoite kummassakin verkkosegmentissä. Datalinkkikerroksella toimiminen aiheuttaa sen, että silloilla voidaan kytkeä yhteen vain samantyyppisiä verkkoja. Silta lukee jokaisen paketin fyysisen osoitteen ja päättää fyysisten osoitteiden taulukkonsa perusteella, ohjataanko paketti toiseen verkkosegmenttiin, vai jätetäänkö paketti ohjaamatta. Mikäli fyysistä osoitetta ei löydy osoitetaulusta, silta suorittaa

yleislähetyksen, eli lähettää paketin kaikkiin liityntöihinsä. Siltojen huonona puolena on se, että kaikista siirroista aiheutuu pieni viive fyysisen osoitteen lukemisen takia, ja vilkkaassa verkossa luenta saattaa aiheuttaa merkittävän hidasteen verkon toimintaan. (Keogh 2001, 103 – 105.)

Kytkimien avulla kytketään verkon päätelaitteet yhteen samaan tapaan kuin älykkäillä keskittimillä. Yhteydet, joissa lähiverkon segmentit ovat yhdistetty keskittimillä ja silloilla, voidaan korvata täysin kytkimellä. Kytkimen avulla mahdollistetaan tehokkaampi liikennöintinopeus kuin keskittimillä ja silloilla toteutetussa lähiverkossa. Yksittäisen portti voi keskittimestä poiketen liikennöidä kaksisuuntaisesti, jolloin voidaan sekä lähettää että vastaanottaa paketteja samanaikaisesti. Kytkimet mahdollistavat lisäksi sen, että verkon törmäysalueiden lukumäärä on yhtä suuri kuin kytkimen porttien lukumäärä. Koska siirtotiellä ei näin ollen tapahdu törmäyksiä, voi kytkin voi tarjota jokaiselle portille portin nimellisnopeuden. Kytkin lukee paketin fyysisen kohdeosoitteen, ja tämän perusteella tarkastaa osoitetaulustaan, mihin porttiin paketti on tarkoitettu. Mikäli kohdeosoite on tuntematon, paketti lähetetään kaikkiin liityntöihin sillan tapaan. Ideaalitapauksessa fyysinen osoite löytyy kytkimen osoitetaulusta ja yhteys avataan vain näiden kahden portin välille siksi aikaa, kunnes paketti on välitetty kytkimen lävitse. (Jaakohuhta 2005, 135 – 139.)

Kytkimen kytkentätavan määrittelyssä käytetään kahta eri menettelytapaa. Nopeammassa tavassa, kytke ja välitä (cut-through), paketin lähetys aloitetaan heti kun kohdeosoite on saatu kytkimen tietoon. Tällöin paketin loppuosa saattaa olla vielä matkalla, mutta kytkemispäätös saadaan tehtyä ennen kuin paketti on kokonaan saapunut kytkimelle. Kytke ja välitä -menettelyn huonona puolena on se, ettei itse paketin sisältöä tarkasteta, jolloin se saattaa olla viallinen. Varastoi ja välitä (store-and-forward) -tavassa saapuva paketti luetaan kokonaan kytkimen puskuriin, paketin eheys tarkastetaan ja vasta tämän jälkeen selvitetään kohdeosoite ja se, mihin porttiin paketti lähetetään. Varastoi ja välitä -menettelyssä viallisten pakettien lukumäärää saadaan pienennettyä, mutta toisaalta myös viiveet suurenevat. Useimmat uudemmat kytkimet osaavat käyttää molempia menettelytapoja esimerkiksi siten, että paketteja välitetään kytke ja

välitä -menetelmällä niin kauan kun virheitä ei synny. Kun virheitä alkaa syntyä, siirrytään varastoi ja välitä -menetelmään, jossa pysytään siihen saakka, kunnes virheiden lukumäärä pienenee. (Jaakohuhta 2005, 139.)

Kytkimen ominaisuuksia kuvaavia ominaisuuksia ovat esimerkiksi kytkimen suodatuskyky, joka ilmaisee sitä, kuinka monta kohdeosoitetta kytkin kykenee lukemaan paketeista määritellyssä aikajaksossa. Välityskyky ilmaisee sitä, kuinka monta pakettia kyetään kytkimen läpi kuljettamaan tietyssä ajanjaksossa. Ruuhka tarkoittaa kytkimessä tilannetta, jolloin yhteen porttiin kohdistuu samanaikaisesti useita liikennöintivirtoja ja portin välityskyky ylitetään. Tällöin ruuhkautunut liikenne puskuroidaan kytkimen puskuriin odottamaan lähetysvuoroaan. Kun ruuhka taas purkautuu, saa lähettäjä lähettää lisää dataa kytkimelle. Tälläistä pakettien ruuhkatilanteen purkamista kutsutaan vuonohjaukseksi, ja vuonohjaus on määritelty IEEE 802.3x –määrittelyssä. (Jaakohuhta 2005, 149 - 150.)

Kytkimen nopean kytkennän mahdollistaa kytkimen taustaväylän nopeus, joka on useimmiten saman verran kuin kytkimen porttien kokonaiskapasiteetti. Teoriassa 24-porttisen 100Mbps kytkimen tulisi pystyä liikennöimään 2400Mbps nopeudella. Tällöin oletetaan, että kytkimen kaikki portit ovat kytkettyinä ja porttien läpi liikennöidään siten, että koko siirtokaista on varattuna. Tämä laskelma ottaa kuitenkin kantaa vain unicast-tyyppiseen pisteestä pisteeseen liikennöintiin. Multicast-tyyppinen liikenne, jossa lähetetään yhdestä pisteestä moneen pisteeseen, kuormittaa kytkimen kapasiteettia huomattavasti enemmän. Näin ollen kytkimen taustaväylän nopeus tulisi suhteuttaa siinä kiinni olevien päätelaitteiden käyttötarkoitukseen. (Jaakohuhta 2005, 153 – 154.)

Kytkinten ansiosta voidaan lähiverkkoon määritellä myös toisistaan erillään olevia ryhmiä, eli virtuaalisia lähiverkkoja (VLAN, Virtual local area network). Virtuaaliset lähiverkot liikennöivät samassa fyysisessä verkossa loogisesti erillään toisistaan. Virtuaaliset lähiverkot on määritelty standardeissa IEEE 802.1Q, IEEE 802.1p ja IEEE 802.1ad. Virtuaalisilla lähiverkoilla saadaan lisättyä lähiverkon tietoturvaa ja tiedonsiirtokapasiteettia, rajoitettua lähiverkkoliikennettä ja levitysviestejä sekä helpotettua ylläpidon tehtäviä käyttäjien siirtyessä fyysisesti

eri alueille. Virtuaalinen lähiverkko voidaan toteuttaa päätelaitteiden MAC-osoitteiden (Media access control) perusteella, kytkimen porttien perusteella, verkko-osoitteen perusteella tai tietoliikenneprotokollan perusteella. (Jaakohuhta 2005, 157.)

Reitittimet eivät sinänsä kuulu lähiverkkojen tekniikkaan, mutta niitä käytetään usein lähiverkoissa virtuaalisten lähiverkkojen yhdistämiseen sekä yhteyden luomiseen lähiverkosta ulospäin. Reititin ei kuitenkaan ole välttämätön virtuaalisten lähiverkkojen yhdistämisessä, vaan reititys voidaan myös tehdä kytkimellä, mikäli kytkimestä löytyy reititinominaisuuksia, joiden avulla virtuaaliset lähiverkon saadaan reititettyä toisiinsa halutusti. (Jaakohuhta 2005, 162 - 163.)

2.2 Lähiverkon kaapelointi

Kaapelointi toimii lähiverkon työasemien, tulostimien, palvelimien ja aktiivilaitteiden yhdistäjänä. Käyttötarkoituksesta riippuen kaapelointi voidaan toteuttaa useilla erilaisilla kaapeleilla ja tekniikoilla. Yhteistä näillä on se, että kaikki noudattavat standardeja. Nykyisin lähiverkkojen kaapeloinnissa käytetään lähes poikkeuksetta yhtä yleiskaapelointistandardiperheen EN 50173 -asennusstandardeista. (Jaakohuhta 2005, 47.)

EN 50173 -standardeissa määritellään, millainen kaapeloinnin tulee olla eri kohteissa, miten se tulee asentaa, ja miten asennukset tulee testata. Suomessa lähiverkon yleiskaapelointistandardina käytetään useimmiten standardia SFS EN 50173-1, joka tunnetaan Suomessa paremmin nimellä yleiskaapelointi. Tässä työssä yleiskaapeloinnilla tarkoitetaan SFS EN 50173-1 -standardin mukaista yleiskaapelointia. Yleiskaapelointijärjestelmä määrittelee toimittajariippumattoman kaapelointijärjestelmän, jossa on yksi tai usempia rakennus samalla alueella. Yleiskaapelointistandardi määrittelee standardit symmetriselle kupari- tai valokuitukaapeloinnille sekä yleiskaapeloinnin rakenteelle ja osille. (Jaakohuhta 2005, 48.)

Yleiskaapeloinnin osat muodostuvat toiminnallisista rakenteista ja osista. Toiminnalliset osat muodostuvat aluekaapeloinnista, nousukaapeloinnista sekä kerroskaapeloinnista. Kaapelointi tarkoittaa yhtä tai useampaa standardin hyväksymää kaapelia. Näistä aluekaapelointi sisältää enimmillään 2000 metriä pitkän kaapeloinnin aluejakamosta yhteen tai useampaan talojakamoon, nousukaapelointi enimmillään 500 metriä pitkän kaapeloinnin talojakamosta yhteen tai useampaan kerrosjakamoon. Kaapeloinnin viimeinen osa, kerroskaapelointi, sisältää enimmillään 90 metriä pitkän kaapeloinnin, ja kerroskaapelointi ulottuu kerrosjakamosta yhteen tai useampaan työpisterasiaan. Aluekaapeloinnissa suositellaan käytettäväksi yksimuotokuitua ja nousukaapeloinnissa monimuotokuitua. Koko siirtokanavan pituus kytkimen portilta työaseman verkkokortille saa olla enintään 100 metriä. Yleiskaapelointistandardi määrittelee siirtotielle taulukon 1 mukaiset vaatimukset, mutta lähiverkoissa käytetään ainoastaan luokkia D, E ja F (Jaakohuhta 2005, 49 - 58.)

TAULUKKO 1. Siirtotien kaapelointiluokat (Jaakohuhta 2005, 60.)

Luokka	Kategoria	Suurin taajuus	Ethernet-sovellus
A	-	100 kHz	-
B	-	1 MHz	-
C	3	16 MHz	10Base-T
D	5	100 MHz	100Base-TX
	5e	125 MHz	1000Base-T
E	6	250 MHz	1000Base-T
F	7	600 MHz	10Gbase-T

Yleiskaapelointistandardi määrittelee itse siirtotielle taulukon 2 mukaiset sähköiset ominaisuudet, jotka koostuvat itse parikaapeleista, liittämistarvikkeita ja jakamoiden sisäisistä kytkentäkaapeleista. (Jaakohuhta 2005, 60.)

TAULUKKO 2. Siirtotien vaaditut sähköiset ominaisuudet (Jaakohuhta 2005, 61.)

Kytkentä	Kaukopään ylikuulumisvaimennus tehosummana [dB/100 m]
Pituus [m]	Vaimennus – ylikuulumissuhde tehosummana [dB/100 m]
Heijastusvaimennus [dB]	Tasavirtasilmukkaresistanssi [S]
Lähipään ylikuulumisvaimennus kahden parin välillä [dB/100 m]	Kulkuaika [Fs]
Lähipään ylikuulumisvaimennus tehosummana [dB/100 m]	Kulkuaikaero [Fs]
Kaukopään ylikuulumisvaimennus kahden parin välillä [dB/100 m]	Vaimennus [dB]

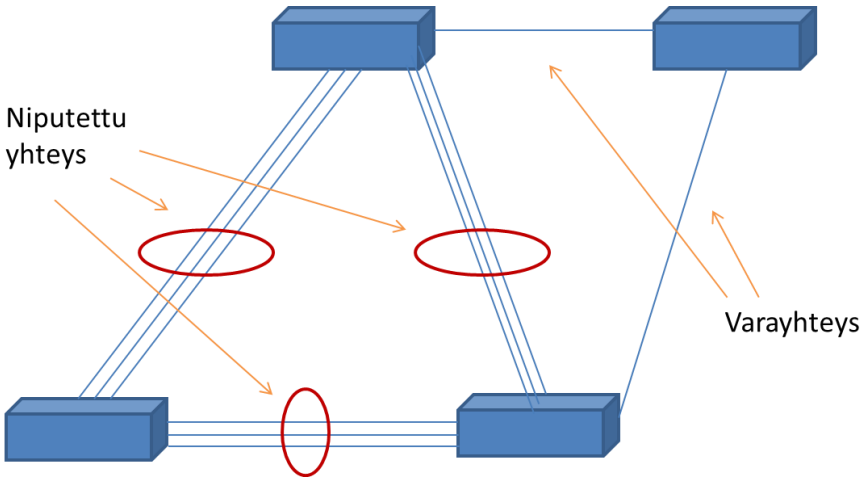
Kaapelointi tulee aina rakentaa siten, että kaapelointi on toteutettu siististi ja dokumentoitu hyvin. Lisäksi on tärkeää, että kaapelointi on rakennettu riittävän kattavasti, jolloin yhden liittimen vikaantuminen ei aiheuta suuria ongelmia käyttäjille. Kaapeliasennuksissa tulee huomioida, että johtotiet eristetään sähköjohdoista, läpivienneistä tehdään riittävän avaria, johdinniput niputetaan siististi, rasiat ja kytkentäpisteet merkitään selvästi ja varayhteyksiä rakennetaan heti alkuun riittävästi. Laitetiloissa on tärkeää, että tilat ovat lukitut, ilmastointi on järjestetty asianmukaisesti, sähköpistokkeita on riittävästi, laitekaapit ovat maadoitettu asianmukaisesti, ja tilat on sijoitettu siten, että laitteiston ylläpitäminen on helppoa. (Jaakohuhta 2005, 69 - 71.)

2.3 Vikasietoinen lähiverkko

Lähiverkon suunnittelussa on tärkeää ottaa huomioon myös verkon vikasietoisuus kokonaisuutena. Fyysistä vikasietoisuutta saadaan lisättyä helpoiten rakentamalla varayhteyksiä verkon aktiivilaitteiden ja palvelinten välille. Varayhteystoimintojen nimitykset vaihtelevat valmistajakohtaisesti, mutta kaikkien toimintaperiaate perustuu yhteyspulsseihin. Laitteiden välille luodaan

kaksi yhteyttä, joista toinen toimii aktiivisena ja toinen varayhteytenä. Aktiivisen yhteyden mukana kulkee yhteyspulsseja, joiden avulla laitteet huomaavat yhteyden olevan kunnossa. Mikäli yhteyspulssit katoavat, otetaan varayhteys käyttöön automaattisesti. (Jaakohuhta 2005, 176 - 177.)

Yhteyksien niputusta voidaan käyttää kahden tai usemman kytkimen välillä siirtokaistan suurentamiseksi ja yhteyksien varmistamiseksi. Yhteyksien niputus on määritelty standardissa IEEE 802.3ad, mutta useilla valmistajilla on kuitenkin omat versionsa luotuna tästä standardista, eivätkä eri valmistajien versiot ole yhteensopivia keskenään. Niputetuissa yhteyksissä liikenne kulkee siten, että jokainen istunto käyttää tiettyä yhteyttä koko istunnon ajan. Toinen istunto saattaa näin ollen käyttää toista yhteyttä oman istuntonsa ajan, jolloin tapahtuu kuormantasausta yhteysnipun fyysisten yhteyksien välillä. Vikasietoisuus on saavutettu yhteyksien niputuksessa siten, että yhden fyysisen yhteyden vikaannuttua kaikki sillä ollut liikenne ohjataan muille fyysisille yhteyksille, ja näin ollen myös itse siirtoyhteys hidastuu. Esimerkki niputetuista- ja varayhteyksistä löytyy kuviosta 1. (Jaakohuhta 2005, 177 - 178.)



KUVIO 1. Esimerkki niputetuista- ja varayhteyksistä.

Vanhin varayhteysmenettely on nimeltään virityspuu (spanning tree). Virityspuumenettely on määritelty standardissa IEEE 802.1D, ja

virityspuumenettelyn avulla saadaan estettyä lähiverkolle vaarallisten silmukoiden syntyminen. Virityspuualgoritmi on yhteensopiva eri laitevalmistajien välillä, ja virityspuualgoritmi sopii hyvin kytkinverkkoon. Virityspuumenettely huolehtii siitä, että kaikkien verkossa toimivien laitteiden välille syntyy vain yksi yhteys. (Jaakohuhta 2005, 183.)

Virityspuumenetelmässä määritellään verkolle juurikytkin, josta kaikki muut laitteet alkavat rakentaa puumaista verkkohierarkiaa. Hierarkiassa laitteiden tasot määräytyvät niiden prioriteetin, edullisimman reitin, välitysviiveen ja MAC-osoitteen perusteella. Virityspuumenetelmä käyttää hyväkseen BPDU-paketteja (Bridge procotol data unit), joiden avulla juurikytkin selvittää verkon tilaa, ja tämän tiedon pohjalta muutoksentarvetta. Kun virityspuumenetelmä on lähiverkossa valmis, mahdollisiin verkonmuutoksiin reagoidaan dynaamisesti ja laitteiden välille lasketaan uudet silmukattomat reitit. (Jaakohuhta 2005, 184.)

Vikatilanteen sattuessa laitteet eivät lähetä hyötyliikennettä niin kauan, kunnes virityspuumenetelmä on laskenut uudet toimivat reitit koko verkolle. Virityspuumenetelmän pahin ongelma onkin hidas uudelleenkytkeytymisaika, joka saattaa olla pahimmillaan 30-90 sekuntia vikatilanteen huomaamisesta. Virityspuumenetelmää on kehitetty toimintaa nopeuttavilla päivityksillä kuten IEEE 802.1w eli RSTP (Rapid spanning tree protocol), joka vähentää verkon uudelleenkytkeytymisajan noin 10 sekuntiin. Usean virtuaalisen lähiverkon sisältävissä lähiverkoissa parannusta tähän on tuonut lisäksi IEEE 802.1s eli MSTP (Multiple spanning tree protocol), jonka avulla voidaan luoda oma virityspuumenetelmä jokaiselle virtuaaliselle lähiverkolle erikseen ja näin ollen pienentää verkkosegmentin kokoa. (Jaakohuhta 2005, 185 - 186.)

3 ETÄYHTEYDET

3.1 TCP/IP-viitemalli

TCP/IP-viitemalli (Transmission control protocol/Internet procotol) on hyvin samankaltainen OSI-mallin (Open systems interconnection) kanssa. OSI-mallista poiketen TCP/IP-viitemallista on neljä mallinnuskerrosta OSI-mallin seitsemän sijaan. TCP/IP-viitemalli kehitettiin ennen OSI-mallia, mutta niiden kerrosten toiminta on hyvin samankaltaista, ja useimmiten kerrokset vastaavat suoraan toisiaan. (Anttila 2000, 35.)

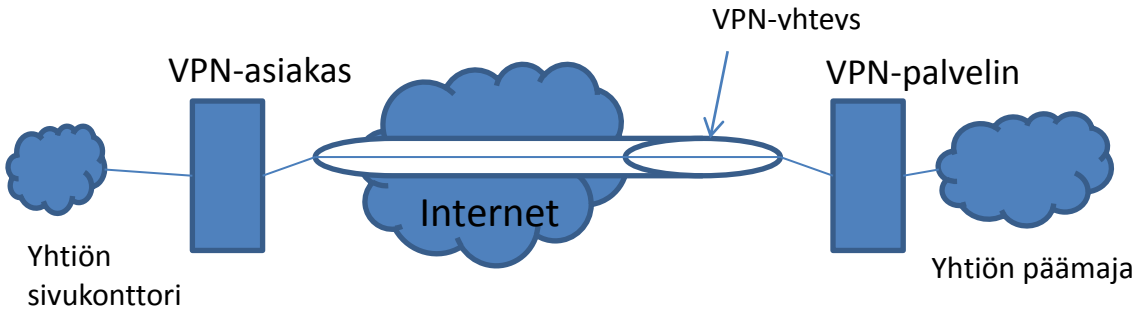
Neljäs kerros toimii sovelluskerroksena. Sovelluskerroksen tehtävänä on tarjota verkkopalvelut, merkistökoodaus sekä toimintojen koordinointi eri laitteiden välillä. Sovelluskerroksella toimivat esimerkiksi sähköprotokollat SMTP (Simple mail transfer protocol) ja POP3 (Post office protocol 3). Kolmas kerros toimii kuljetuskerroksena. Kuljetuskerros huolehtii datan asettelusta oikeankokoisiin palasiin, jotka voidaan myöhemmin lähettää vastaanottajalle. Kolmannella kerroksella toimivat protokollat TCP (Transmission control protocol) sekä UDP (User datagram protocol). (Anttila 2000, 32 - 34.)

Toinen kerros on verkkokerros. Verkkokerroksen tehtävänä on pakata kolmannelta kerrokselta saadut paketit ja välittää ne oikealle vastaanottajalle vastaanottajan osoitteen perusteella. Toisella kerroksella toimivat esimerkiksi protokollat IP (Internet protocol), ICMP (Internet control message protocol) sekä IGMP (Internet group management protocol). Alin eli ensimmäinen kerros on nimeltään fyysinen kerros. Fyysisen kerroksen tehtävänä on pakata verkkokerrokselta saatu data paketteihin, joiden otsikoista löytyy vastaanottajan ja lähettäjän verkkokortin fyysinen osoite. Tämän jälkeen fyysinen kerros muuntaa bitit sähköisiksi signaaleiksi ja lähettää ne siirtotielle. (Anttila 2000, 34 - 35.)

3.2 Lähiverkkojen yhdistämistekniikat

Helpoin tapa yhdistää lähiverkot toisiinsa on käyttää hyväkseen operaattorin tarjoamaa yhdistämispalvelua. Tällöin operaattorille maksetaan kuukausittainen maksu verkkojen yhdistämisestä, ja teknisen puolen yhdistämisestä hoitaa kokonaan operaattori. Useimmiten palvelu toteutetaan käyttämällä operaattorin omaa MPLS-verkkoa (Multiprotocol label switching), jonka läpi luodaan salattu tunneli kahden lähiverkon välille. Asiakkaan jokainen toimipiste varustetaan reitittimellä, johon toimipisteen lähiverkko yhdistetään. Huonona puolena operaattorin yhdistämispalvelussa on kiinteä kuukausimaksu. (IP VPN 2009.)

Lähiverkot yhdistetään internetin yli käyttäen VPN-yhteyksiä. Tällöin riittää, että jokaisella yrityksen toimipisteellä on esimerkiksi paikallisen operaattorin tarjoama internet-yhteys. Yhdessä toimipisteessä sijaitsee VPN-palvelin, johon muut toimipisteet ottavat yhteyden omalla VPN-asiakaspalvelimellaan. Kuten kuviosta 2 nähdään, toimipisteiden välinen yhteys luodaan turvattoman internetin ylitse salatulla VPN-yhteydellä, jolloin yhteyttä voidaan pitää turvallisina. (VPN Overview 2009.)



KUVIO 2. Esimerkki lähiverkkojen yhdistämisestä Internetin yli

Yhdistettäessä lähiverkot olemassa olevan puhelinverkon yli käytetään hyväksi paikalliselta puhelinyhtiöltä vuokrattuja kuparipareja, jotka yhdistetään toisiinsa puhelinyhtiön toimesta. Tällöin puhutaan pisteestä pisteeseen yhteydestä, jota voidaan pitää turvallisimpana ratkaisuna verkkojen kytkemisessä. Pisteestä

pisteeseen yhteys on paras valinta silloin, kun toimipisteet sijaitsevat samassa kaupungissa lähellä toisiaan. Verkotettaessa useita toimipisteitä toisiinsa ratkaisu on huono, koska yhteyksiä tulee nopeasti useita kymmeniä. Yhteyksien lukumäärä saadaan kaavasta N(N-1) / 2. Tällöin esimerkiksi viiden toimipisteen yhdistämisessä toisiinsa tarvitaan 5*(5-1) / 2 = 10 eri pisteestä pisteeseen yhteyttä. (Anttila 2000, 40 - 41.)

Mikäli lähiverkot sijaitsevat lähellä toisiaan, niin ne voidaan yhdistää myös langattomasti WLAN (Wireless local area network)-tekniikalla. Tällöin molempiin rakennuksiin asetetaan WLAN-sillat, jotka yhdistetään kyseenomaisten rakennuksen lähiverkkoon. Huonona puolena langattomassa yhdistämisessä on häiriöalttius sekä sen vaatimat lyhyet välimatkat. (Understanding wireless LAN bridges 2009.)

3.3 VPN

3.3.1 VPN-yhteydet ja yhteysmuodot

VPN tarkoittaa yleisesti kahden verkon tai asiakkaan ja verkon yhdistämistä toisiinsa virtuaalisella salatulla tunnelilla. Tämä virtuaalinen tunneli luodaan jonkin turvattoman verkon ylitse, joka on useimmiten internet. VPN ei vielä itsessään määritä, millä protokollalla yhteys tunneloidaan ja minkä siirtymäverkon yli yhteys tunneloidaan. VPN:n tunnelointitavan valitsee VPN-verkon suunnittelija. (VPN-verkot 2009.)

VPN:llä voidaan rakentaa kolmenlaisia yhteysmuotoja: kahden lähiverkon yhdistäminen, asiakkaan ja lähiverkon yhdistäminen sekä asiakkaan ja asiakkaan yhdistäminen. Tässä työssä keskitytään verkkojen yhdistämiseen, johon on kaksi eri vaihtoehtoista tapaa riippuen verkon rakenteesta. (VPN-verkot 2009.)

Mikäli verkot voidaan yhdistää reitittimillä, on helpointa rakentaa VPN-yhteys suoraan reitittimien välille. Tätä tapaa käyttävät muun muassa operaattorit, jotka omistavat oman runkoverkon. Mikäli lähiverkot sijaitsevat kaukana toisistaan ja

halutaan luoda yhteys internetin yli, on helpointa asentaa lähiverkkoihin erilliset tietokoneet, jotka luovat niiden välille salatun tunnelin internetin ylitse. Tätä tapaa käytettäessä tulee suunnittelijan valita VPN-yhteydelle sopiva tunnelointitapa. (VPN-verkot 2009.)

3.3.2 VPN-yhteyksien tunnelointitavat

IPsec (Internet protocol security) on joukko yhteysprotokollia, joiden avulla saadaan lähiverkot kytkettyä keskenään toisiinsa. IPsec tukee muun muassa eheyden tarkistusta, yhteyden todentamista sekä pääsynvalvontaa. IPsec koostuu noin 40 RFC-dokumentista (Request for comments), joissa kuvataan sen toimintaa ja ominaisuuksia. IPsec käyttää pääsynvalvontaprotokollanaan IKE (Internet key exchange)-protokollaa, jonka avulla käyttäjän todennus voidaan toteuttaa etukäteen jaetun avaimen, julkisen avaimen, RADIUS-palvelimen (Remote authentication dial in user service) tai etukäteen jaetun sertifikaatin avulla. (How Virtual Private Networks Work 2009.)

IPsec tukee pakettikohtaista salausta AH (Authentication Header) ja ESP (Encapsulating security payload) protokollien avulla. Niitä voidaan käyttää joko erikseen tai yksitellen. (RFC2402 2009; RFC2406 2009.)

PPTP (Point to Point Tunneling Protocol) on Microsoftin kehittämä tunnelointiprotokolla, jonka avulla voidaan toteuttaa VPN-yhteys asiakkaan ja palvelimen välillä esimerkiksi internetin yli. PPTP käyttää TCP-porttia 1723 eikä toimi NAT:n (Network address translation) lävitse. PPTP ei itsessään salaa liikennettä, mutta sen kanssa käytetetään usein MPPE-protokollaa (Microsoft Point-to-Point Encryption), jonka avulla yhteys voidaan luoda 128-bittisellä salauksella. (PPTP Introduction 2009; How Virtual Private Networks Work 2009.)

PPTP käyttää tiedonsiirrossa hyväkseen kahdenmallisia pakettityyppejä. Datapaketit muodostuvat varsinaisesta käyttäjädatasta, ja käyttäjädata on

kapseloitu GRE -protokollan (Generic routing protocol) avulla. Valvontapaketit sisältävät valvontaviestejä, joita käytetään tunnelin merkinantoon ja tilatiedostoon. Valvontapaketit käyttävät hyväkseen asiakkaan ja palvelimen välille muodostettua TCP -istuntoa. (Perlmutter & Zarkower 2001, 116.)

L2TP (Layer 2 tunnel protocol) on L2F -protokollan (Layer 2 forwarding) seuraaja, jossa on parannetut tietoturvaominaisuudet. L2TP toimii TCP/IP-viitemallin toisella kerroksella, ja L2TP:n toiminta perustuu ohjausviesteihin ja informaatioviesteihin. Ohjausviestit huolehtivat tunnelin luonnista, ylläpidosta ja sen lopettamisesta. L2TP:ssä autentikointi tapahtuu etukäteen määritetyn salasanan avulla, ja L2TP käyttää oletuksena UDP-porttia 1701. Koska L2F-protokolla käyttää oletuksena samaa porttia, L2TP:n otsikossa on versiokentässä luku kaksi.
(RFC2661 2009.)

L2TP ei tarjoa pakettitason suojausta, vaan L2TP:n kanssa käytetään useimmiten IPsec-protokollaperheen ESP- tai AH-protokollia. Tällöin avataan IPsec -tunneli ja avataan L2TP-tunneli sen sisälle. Tämä tehdään sen takia, että nykyiset käyttöjärjestelmät eivät nykyisin tue suoraan pelkästään IPsec-tunnelointia vaan ne vaativat L2TP-protokollan käyttöä. IPsec lisää tietenkin samalla tuen käytönvalvontaan, jolloin paketteja voidaan suodattaa tehokkaasti esimerkiksi IP-osoitteen perusteella. (RFC2661 2009.)

VTUN (Virtual tunnel) on tunnelointitapa, jonka avulla VPN-yhteys voidaan muodostaa TCP/IP-verkoissa unix/linux-palvelimien välille ja näin yhdistää lähiverkot keskenään. VTUN ei käytä hyväkseen mitään tunnetuista tunnelointiprotokollista vaan luottaa omaan protokollaansa, joka käyttää TCP- tai UDP -yhteyksiä. VTUN luo IP-, PPP- (Point-to-Point protocol), SIP- (Session initiation protocol) tai Ethernet-tunnelin, joka voidaan lisäksi pakata ja salata. Yhteys salataan vain BlowFish-algoritmin avulla, ja kirjautuminen 128-bittisen MD5:n (Message digest 5) avulla, joten VTUN:n kehittäjät suosittelevat tunnelin luomista esimerkiksi SSH-yhteyden (Secure shell) lävitse, jolloin yhteys on turvallisesti salattu. (VTUN FAQ 2009.)

SSL VPN (Secure socket layer virtual private network) eroaa muista tunnelointitavoista siinä, että SSL VPN toimii TCP/IP-viitemallin kerroksilla kolme ja neljä. SSL VPN -ohjelmistot eivät ole yhteensopivia PPTP, L2TP tai IPsec-tunnelointitapojen kanssa. SSL VPN:ää ei ole standardoitu, joten sen määritykset riippuvat käytettävästi ohjelmistosta. Yleisesti SSL VPN käyttää kuitenkin TLS-protokollaa (Transport layer security) yhteyden luomiseen, salaamiseen ja ylläpitoon. Yksi käytetyimmistä SSL VPN ohjelmistoista on OpenVPN, jonka avulla voidaan yhdistää lähiverkot toisiinsa käyttäen hyväksi OpenSSL-kirjastolla luotuja RSA-sertifikaatteja ja etukäteen määritettyjä salasanoja. OpenVPN toimii kaikissa yleisimmissä käyttöjärjestelmissä ja on ilmainen. (OpenVPN Overview 2009.)

4 PALVELIMET

4.1 Palvelinvirtualisointi

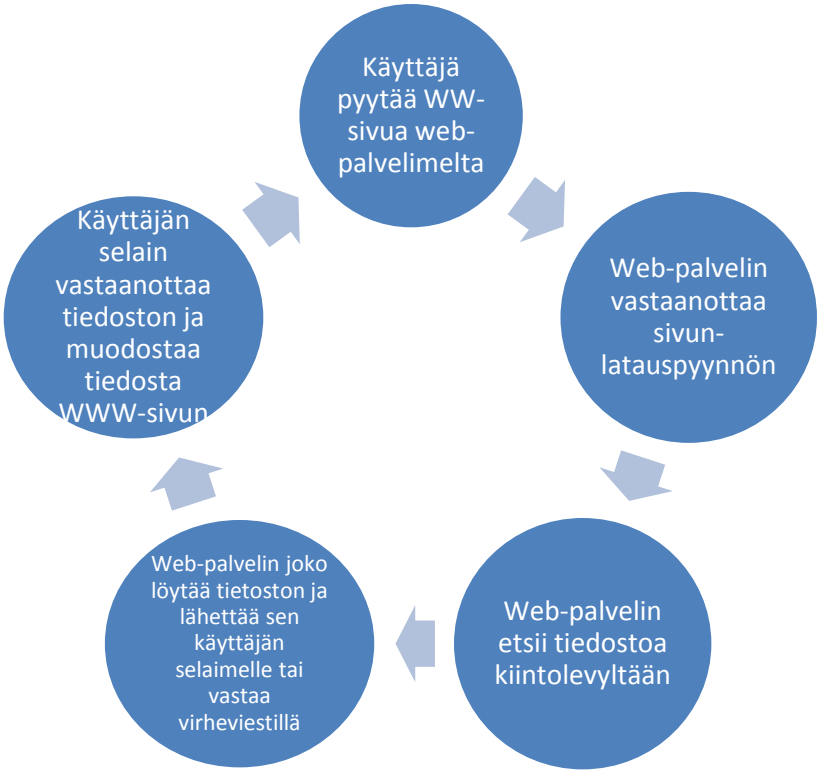
Palvelinohjelmistoja voidaan asentaa joko yksittäisille fyysisille tietokoneille tai virtualisoiduille virtuaalikoneille. Usein palvelimelle asennetaan vain yksi palvelu, jolloin laitteiston resurssit jäävät suurelti osin käyttämättä. Kun käytetään palvelinvirtualisointia, voidaan yhdelle ja samalle koneelle asentaa virtuaalisesti monta virtuaalikonetta, jolloin palvelimen käyttöastetta saadaan kasvatettua tehokkaasti. Asennetuille virtuaalikoneille voidaan varata juuri sen verran resursseja, kun ne tarvitsevat toimiakseen. Tämän johdosta tarvitaan vähemmän fyysistä palvelinlaitteistoa ja laitteiston hallinta helpottuu ylläpitäjän kannalta. (Virtualisointi 2011.)

Laitteistovirtualisoinnissa virtuaalikone on ohjelmistosäiliö, jossa voidaan ajaa käyttöjärjestelmiä ja ohjelmia siten, kuin ne olisivat ajettavana oikeassa tietokoneessa. Käyttöjärjestelmän kannalta virtuaalikone ei eroa normaalista fyysisestä tietokoneesta mitenkään, vaan se sisältää samat komponentit kuin normaali tietokonekin. Tämän johdosta virtuaalikoneiden avulla saavutetaan hyvä yhteensopivuus kaikkien x86-tietokoneiden kanssa, virtuaalikoneet saadaan eristettyä toisistaan täysin ohjelmallisesti, eivätkä virtuaalikoneet ole riippuvaisia itse laitteistosta, jonka päällä ne toimivat. Virtuaalikoneet on paketoitu niin, että niitä voidaan helposti kopioida ja siirtää paikasta toiseen esimerkiksi Internetin tai kannettavan kiintolevyn avulla. (Virtualization Basics. 2011.)

4.2 WWW-palvelimet

WWW-palvelimen (World wide web) tehtävänä on tarjoille WWW-sivuja niitä pyytäville web-selaimille. Käyttäjän selatessa internetiä WWW-palvelimen osoitteella WWW-palvelin saa sivunlatauspyynnön, minkä jälkeen WWW-palvelin yrittää etsiä kiintolevyltään käyttäjän haluaman tiedoston ja palauttaa tiedoston onnistuessaan käyttäjän internet-selaimelle, joka muodostaa siitä

WWW-sivun. WWW-selaimen toiminta käy ilmi alla olevasta kuviosta 3. (What is web server. 2011.)



KUVIO 3. Web-palvelimen toimintaperiaate

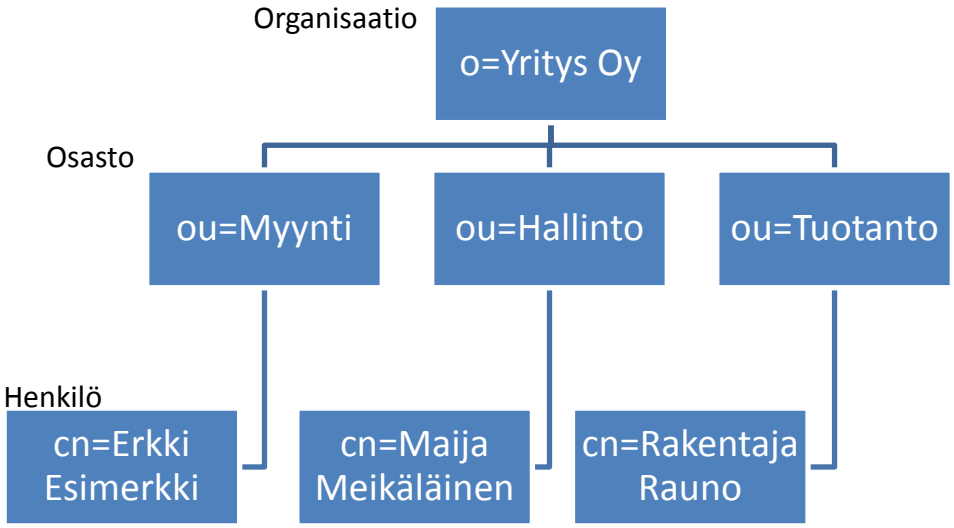
Tilastollisesti yleisimmin käytetyt WWW-palvelimet ovat Apache sekä IIS (Internet Information Services) (November 2010 Web Server Survey. 2010). Apache on avoimeen lähdekoodiin perustuva web-palvelin, joka tukee oletuksena ainoastaan staattisten tiedostojen jakamista. Apache on kuitenkin laajennettavissa moduuleilla, joiden avulla palvelinta voidaan räätälöidä omia tarpeita vastaavaksi. Moduuleiden avulla Apachella pystyy suorittamaan esimerkiksi PHP-, Perl-, Python-, ja Tcl-kielillä kirjoitettua koodia. Muita moduuleilla saavutettavia ominaisuuksia ovat muun muassa SSL- ja TLS-suojaukset, URL-osoitteen uudelleenkirjoitus, erilaiset autentikaatiomenetelmät sekä tiedostojen pakkausmenetelmät. Apache on saatavissa useille käyttöjärjestelmille kuten Unix, GNU, FreeBSD, Linux, Solaris, Novell NetWare, AmigaOS, Mac OS X ja Microsoft Windows. (Wikipedia 2011c.)

Microsoftin IIS 7.5 sisältyy Microsoftin Windows Server 2008 –käyttöjärjestelmiin, ja sen avulla voidaan toteuttaa normaalien WWW-sivujakojen lisäksi WebDAV (Web-based Distributed Authoring and Versioning) ja FTP-jakoja (File transfer protocol). IIS 7.5 –version uusina ominaisuuksina ovat lisäksi sivupyyntöjen suodatus sekä ylläpitoa helpottavat työkalut. Sivupyyntöjen suodatuksen avulla ylläpitäjä voi ennaltamääritellä ja estää haitallisiksi koetut sivupyynnöt kokonaan. Uusiin ylläpitäjän työkaluihin kuuluva Best Practices Analyzer, jonka avulla ylläpitäjä voi tarkastaa IIS-palvelimen asetustiedoston mahdolliset ongelmakohdat. (Web Server (IIS) Role Overview. 2011.)

4.3 Hakemistopalvelimet

Hakemistonpalvelimen tehtävänä on tarjota tietokanta jota voidaan lukea, selata ja josta voidaan etsiä sinne etukäteen tallennettua tietoa. Hakemistot ovat usein yksinkertaisia, ja ne on optimoitu nopeaa tiedonlukua varten, eivätkä hakemistot tue monimutkaisia päivitystoimenpiteitä. Hakemistorakenteet voivat olla paikallisia tai globaaleja riippuen siitä, sallitaanko niiden käyttö pelkästään yhdelle tietokoneelle vai esimerkiksi koko maailmalle. Globaaleiden hakemistorakenteiden erikoispiirteenä on usein myös se, että niissä sijaitseva tieto on hajautettuna useille eri koneille, minkä ansiosta sama tieto on usealla koneella yhtäaikaisesti. (Introduction to OpenLDAP Directory Services. 2011.)

OpenLDAP on ohjelmistoperhe, jonka avulla voidaan hallita LDAP-hakemistopalvelua (Lightweight Directory Access Protocol) useilla eri käyttöjärjestelmillä. LDAP toimii TCP/IP-protokollan päällä, ja LDAP:ssa sijaitseva tieto pohjautuu alkioihin (entries), jotka sisältävät erilaisia attribuutteja, joilla jokaisella on oma tyyppinsä sekä vähintään yksi arvo. Jokaisella alkiolla on lisäksi oma alkion yksilöivä DN-nimi (Distinguished Name), jonka avulla alkio löydetään hakemistosta. Kuten kuviosta 4 voidaan todeta, perinteisesti LDAP-hakemistorakenteessa tieto rakentuu hierarkiseen puumuotoon, joka on usein muodostettu yrityksen organisaatiorakenteen pohjalta. (Introduction to OpenLDAP Directory Services. 2011.)



KUVIO 4. LDAP-tietorakenteen perinteinen rakenne.

Microsoftin Windows Server käyttöjärjestelmistä löytyvä Active Directory eli aktiivihakemisto on käyttäjien ja muiden verkossa olevien toimialueresurssien hallintapiste. Aktiivihakemistossa sijaitsevat esimerkiksi kaikkien käyttäjien tunnukset, salasanat sekä verkon resurssien käyttöoikeusmäärittelyt. Resurssien käyttöoikeusmäärittelyitä voidaan käyttää hyväksi esimerkiksi tiedostojakojen, tulostimien ja muiden verkon laitteiden käyttöoikeuksien hallinnoimisessa. Aktiivihakemisto käyttää avoimia DNS- (Domain name system) ja LDAP-standardeja, joten aktiivihakemiston tietoja voidaan käyttää hyväksi kaikissa näitä standardeja tukevissa laitteissa. (Active Directory. 2011.)

4.4 Nimipalvelimet

Lähiverkon käyttäjälle on mielekästä saada yhteys haluamaansa lähiverkon palveluun käyttäen hyväksi helposti muistettavia osoitteita sen sijaan, että käyttäjä kirjoittaisi esimerkiksi IP-osoitteen selainkentän osoiteriville halutessaan tietylle WWW-sivulle. Lähiverkosta löytyvä DNS-, eli nimipalvelu ratkaisee ongelman

muuntamalla nimet IP-osoitteiksi ja IP-osoitteet nimiksi. Näin ollen käyttäjän ei tarvitse muistaa monimutkaisia IP-osoitesarjoja, vaan riittää, että käyttäjä muistaa palvelulle annetun nimen. Käytännössä tälläinen toteutus voitaisiin toteuttaa asettamalla jokaisen työaseman host-tiedostoon IP-osoite-nimi-parit joita lähiverkossa käytetään, mutta päivitettävyyden kannalta ratkaisusta tulisi usein liian monimutkainen. (Hakala & Vainio 2005, 185 – 186.)

Mikäli lähiverkossa on käytössä ainoastaan Windows-pohjaisia tietokoneita, voidaan nimipalvelu toteuttaa myös NetBIOS-nimien (Network basic input/output system) avulla. Microsoftin NetBios-nimipalvelu on nimeltään WINS (Windows Internet Name Services).

Vain TCP/IP-protokollaa käyttävissä Windows-verkoissa verkon selauspalvelu toimii ainoastaan NetBIOS-nimien pohjalta, jolloin koko selauspalvelun toimivuus on riippuvainen WINS-palvelimen toiminnasta, eli siitä, pystytäänkö verkon NetBIOS-nimet muuntamaan IP-osoitteiksi. NetBIOS-nimipalvelussa tietokoneet ilmoittavat nimensä WINS-palvelimelle rekisteröintipyyntöviestillä, joka sisältää koneen IP-osoitteen sekä NetBIOS-nimen. Saatuaan rekisteröintipyynnön palvelin vastaa nimenrekisteröintivastauksella, joka sisältää WINS-palvelin IP-osoitteen, rekisteröidyn nimen sekä rekisteröinnin voimassaoloajan, jonka jälkeen kyseinen rekisteröinti uusitaan.

NetBIOS-nimipalvelun avulla käyttäjä voi hakea kohdekoneen IP-osoitteen suorittamalla nimikyselyn, minkä tulos tallentuu käyttäjän tietokoneen välimuistiin mahdollistaen myöhemmän NetBIOS-kyselyn tarpeettomuuden. Mikäli WINS-palvelin ei osaa vastata kyselyyn, levittää käyttäjän tietokone kyselyn levitysviestinä lähiverkkoon. (Hakala & Vainio 2005, 209 – 210)

Laajimmin internetissä käytetty nimipalvelin on nimeltään BIND (Berkeley internet name domain). BIND:in kehitystyö aloitettiin 1980-luvun alussa, ja nykyään BIND:iä ylläpitää ja kehittää Internet Systems Consortium. BIND on saatavissa kaikille uusimmille Unix- ja Windows-pohjaisille käyttöjärjestelmille

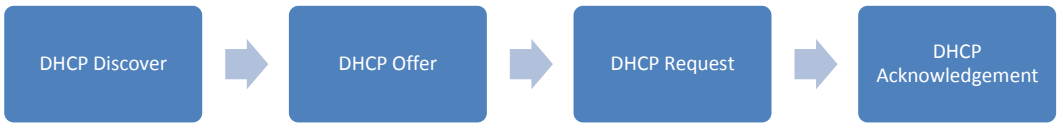
ja BIND tukee LDAP-, Berkeley DB-, PostgreSQL-, Mysql- ja ODBC-tietokantoja. (Wikipedia 2011a.)

BIND:in jälkeen yleisimmin Internetissä käytössä oleva DNS-palvelin on Microsoft Server käyttöjärjestelmistä löytyvä DNS-palvelu, joka tarjoaa kaikki yleisimmin käytetyt DNS-palvelut. BIND:in tapaan DNS-huomautuspalvelun avulla DNS-tietueet saadaan siirrettyä välittömästi toissijaisille DNS-palvelimille kun pääpalvelimen DNS-tietueet muuttuvat. Microsoftin DNS-palvelin tukee useita tietokantoja DNS-tietueiden tallentamiseen, tai DNS-tietueet voidaan tallentaa suoraan Microsoftin Serverillä sijaitsevaan aktiivihakemistoon. Mikäli DNS-tietueet tallennetaan aktiivihakemistoon, voidaan niitä muuttaa, lisätä, tai poistaa kaikilta alueella toimivilta aktiivihakemistopalvelimilta. (Wikipedia 2011b.)

4.5 DHCP-palvelimet

Mikäli lähiverkosta ei löydy DHCP-palvelua (Dynamic host configuration protocol), joudutaan kaikille verkon laitteille määrittämään kiinteät IP-osoitteet erikseen, eli DHCP-palvelu toimii lähiverkon IP-osoitteiden jakelijana. IP-osoitteiden lisäksi DHCP-palvelun avulla voidaan välittää käyttäjille lähes kaikkien TCP/IP-lähiverkossa tarvittavien palvelimien osoitetiedot ja asetukset. (Hakala & Vainio 2005, 211.)

IP-osoitetta tarvitseva laite lähettää lähiverkkoon DHCP Discover levitysviestin, jolla se pyytää IP-osoitetta miltä tahansa DHCP-palvelimelta. Kaikki lähiverkon DHCP-palvelimet vastaavat tähän Discover –viestiin DHCP Offer viestillä, joka on osoitettu vain IP-osoitteen pyytäjälle ja joka sisältää IP-osoitteen sekä tarjouksentekijän IP-osoitteen. Mikäli IP-osoite käy osoitetta pyytävälle laitteelle, lähettää laite DHCP Request –levitysviestin, josta löytyy osoitetta tarjoavan palvelimen IP-osoite. Lopuksi osoitetta tarjonnut palvelin lähettää laitteelle DHCP Acknowledgement –kuittausviestin jolla osoitelainaus kuitataan. DHCP-palvelun viestit on kuvattu kuviossa 5. (Hakala & Vainio 2005, 211 – 212.)



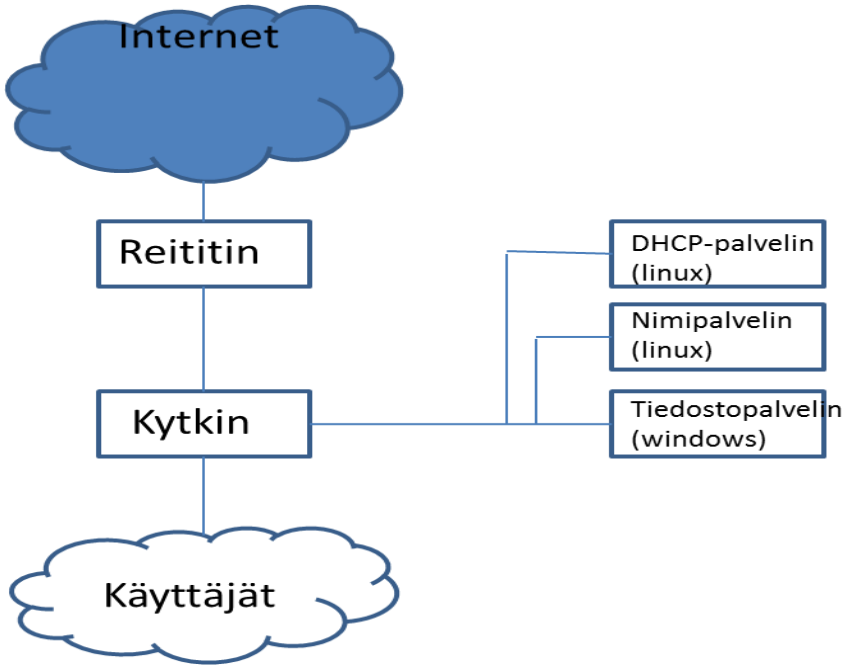
KUVIO 5. DHCP-palvelun viestit

DHCP-palvelu sisältää myös normaalista toiminnasta poikkeavat DHCP Decline ja DHCP Not Acknowledged viestit, joiden avulla ilmaistaan virheen syntyminen. DHCP Decline viestillä laite ilmoittaa palvelimelle tarjotun IP-osoitteen olleen virheellinen, ja DHCP Not Acknowledged viestillä palvelin ilmoittaa laitteelle osoitepyynnön eväämisestä. DHCP-palvelin antaa laitteelle IP-osoitteen vain etukäteen määritellyksi ajaksi, minkä jälkeen vuokrauspyyntö tulee uudistaa käyttäen DHCP Request –pyyntöä ennen vuokrausajan päättymistä. (Hakala & Vainio 2005, 212.)

5 TIETOVERKON DOKUMENTOINTI

Tietoverkon dokumentointi koostuu neljästä erilaisesta dokumenttityypistä jotka kuvaavat verkon toiminnallisuuksia eri tavoin. Dokumentoinnin osa-alueet ovat looginen dokumentointi, fyysinen dokumentointi, laitteiden ja kaapeleiden nimeäminen sekä yksityiskohtainen dokumentointi. (Feldman 1999, 28 - 29.)

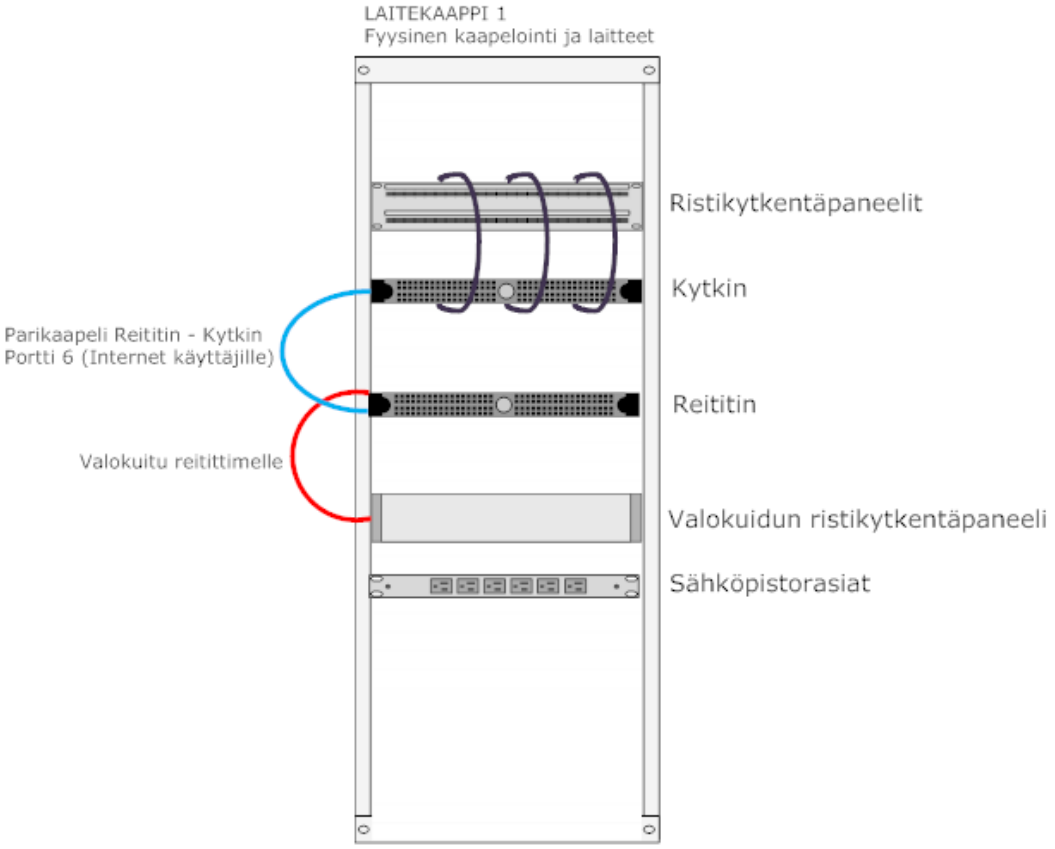
Loogisessa eli toiminnallisessa dokumentoinnissa annetaan yleiskuva verkon segmenteistä, palvelimista, reitittimistä sekä muista verkon toiminnan kannalta tärkeistä asioista. Loogiseen dokumentointiin ei lisätä yksityiskohtaisia tietoja verkosta, vaan verkon osat esitetään esimerkiksi yksinkertaisina laatikoina, jotka yhdistetään toisiinsa viivojen avulla. Loogisen dokumentoinnin tärkein tehtävä on selkeyttää ylläpitäjälle sitä, mitä palveluita mikäkin verkon osa tuottaa ja mitä kautta palvelut välitetään käyttäjille. Esimerkki loogisesta dokumentoinnista esitetään kuviossa 6. (Feldman 1999, 28 - 29.)



KUVIO 6. Esimerkki loogisesta verkon dokumentaatiosta.

Fyysisessä dokumentoinnissa annetaan tarkka ja yksityiskohtainen kuvaus verkon fyysisestä rakenteesta, kaapeloinnista sekä työasemista esimerkiksi rakennuksen pohjakuvaan tai laitekaappia kuvaavaan kuvaan piirrettynä. Fyysisen

dokumentoinnin tarkoituksena on esittää lukijalle, kuinka verkko on tosiasiassa kytketty. Koska fyysisestä dokumentaatiosta käyvät ilmi kaikki kaapelit, työasemat, kirjoittimet ja kytkimet, suositellaan fyysistä dokumenttia tehtäväksi erikseen jokaisesta rakennuksen kerroksesta tai siivestä. Fyysiseen dokumentointiin kuuluvat myös esimerkiksi taulukot, joissa esitetään missä kytkimen portissa työasema on kytkettynä, mikä työaseman verkkokortin MAC-osoite on ja mikä on työaseman fyysinen sijainti rakennuksessa. Esimerkki fyysisestä dokumentoinnista on kuviossa 7 sekä taulukossa 3. (Feldman 1999, 28 - 31.)



KUVIO 7. Esimerkki laitekaapin sisältöä kuvaavasta dokumentoinnista.

TAULUKKO 3. Esimerkki kytkimien porttikytkentöjen dokumentoinnista.

Kytkimien porttikytkennät Osakeyhtiö Oy
Päiväys: 12.2.2011

Laite: Kytkin1
Sijainti: Laitekaappi, ATK-luokka A

Portti	Laite/Isäntänimi	MAC-osoite	IP-osoite	Sijainti	Lisätiedot
1	PC1	00-17-C4-CA-91-CA	10.10.10.11	ATK-luokka	
2	PC2	00-17-C4-CA-91-CB	10.10.10.12	ATK-luokka	
3	PC3	00-17-C4-CA-91-CC	10.10.10.13	ATK-luokka	
4	PC4	00-17-C4-CA-91-CD	10.10.10.14	ATK-luokka	
5	PC5	00-17-C4-CA-91-CE	10.10.10.15	ATK-luokka	
6	PC6	00-17-C4-CA-91-CF	10.10.10.16	ATK-luokka	
7	PC7	00-17-C4-CA-91-CE	10.10.10.17	ATK-luokka	
8	PC8	00-17-C4-CA-91-CG	10.10.10.18	ATK-luokka	
9	PC9	00-17-C4-CA-91-CH	10.10.10.19	ATK-luokka	
10	Tulostin	00-17-C4-CA-91-CI	10.10.10.20	ATK-luokka	
11	Palvelin	00-17-C4-CA-91-CJ	10.10.10.5	ATK-luokka	
12	Pääkytkin	00-17-C4-CA-91-CK	10.10.10.2	ATK-tila	

Laitteiden ja kaapeleiden nimeäminen selkeyttää vianhakua merkittävästi. Nimilapun puuttuminen kaapelista tai laitteesta saattaa hidastaa vianhakua, mikäli korjaaja joutuu etsimään jokaista kaapelia ja laitetta erikseen. Laitteet tulee nimetä lyhyesti ja selkeästi nimellä, joka tulee ilmi suoraan loogisesta ja fyysisestä dokumentaatiosta. Kytkentäkaapeleiden molempiin päihin tulisi liittää nimilappu, josta ilmenee, mitkä laitteet kyseinen kaapeli yhdistää. Tällä tavoin laitekaapista on helppoa ja nopeaa paikallistaa tietty kaapeli esimerkiksi vianhakua varten. (Feldman 1999, 33 - 35.)

Yksityiskohtien dokumentoinnilla täydennetään dokumentointia dokumentoimalla järjestelmäasennusten kuvaukset, asetustiedostot sekä yleisimmät vianetsintäkäytännöt. Näiden avulla helpotetaan vianetsintää sekä mahdollisia laitteiden uudelleenasentamisia. Vianetsintäkäytäntöihin kannattaa kirjoittaa ylös myös kaikki tehdyt järjestelmämuutokset, joiden avulla voidaan helpostit tutkia, mitä järjestelmälle on tehty ja voidaanko ongelma ratkaista yksinkertaisesti kumoamalla tämä muutos. Yksityiskohtaiseen dokumentointiin voidaan liittää

myös esimerkiksi muistilappuja, jotka auttavat vianetsinnässä muita ylläpitäjiä. (Feldman 1999, 36.)

6 YRITYKSEN TIETOVERKON UUDISTAMINEN

Käytännön osuus on poistettu koska sitä ei haluttu julkaista julkisesti.

LÄHTEET

Active Directory. 2011. ITPro.fi [viitattu 12.2.2011]. Saatavissa: http://itpro.fi/wiki/sivut/Identiteetti%20ja%20hakemistot/Active%20Directory.aspx

Anttila, A. 2000. TCP/IP-tekniikka. Juva: WSOY.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: WS Bookwell.

How Virtual Private Networks Work. 2008. Cisco [viitattu 13.12.2009]. Saatavissa: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml

Introduction to OpenLDAP Directory Services. 2011. OpenLDAP [viitattu 22.2.2011]. Saatavissa: http://www.openldap.org/doc/admin23/intro.html

IP VPN. 2009. TDC Business [viitattu 13.12.2009]. Saatavissa: http://tdc.fi/element.php?dogtag=tdcf_ratkaisut_data_ipvpn

Nimipalvelun toiminta. 2011. CSC . Tieteen tietotekniikan keskus [viitattu 12.2.2011]. Saatavissa: http://www.csc.fi/hallinto/funet/palvelut/dns/dns

November 2010 Web Server Survey. 2010. Netcraft [viitattu 12.2.2011]. Saatavissa: http://news.netcraft.com/archives/2010/11/05/november-2010-web-server-survey.html

OpenVPN Overview 2009. 2009. OpenVPN [viitattu 13.12.2009]. Saatavissa: http://openvpn.net/index.php/open-source/245-community-open-source-software-overview.html

PPTP Introduction. 2009. Cisco [viitattu 13.12.2009]. Saatavissa: http://www.cisco.com/en/US/tech/tk827/tk369/tk529/tsd_technology_support_sub-protocol_home.html

Perlmutter, B. & Zarkower, J. 2001. Virtuaaliset yksityisverkot. Helsinki:Edita Oyj.

RFC2341. 2009. IETF[viitattu 13.12.2009]. Saatavissa: http://www.faqs.org/rfcs/rfc2341.html

RFC2402. 2009. IETF [viitattu 13.12.2009]. Saatavissa: http://tools.ietf.org/html/rfc2402

RFC2406. 2009. IETF [viitattu 13.12.2009]. Saatavissa: http://tools.ietf.org/html/rfc2406

RFC2661. 2009. IETF[viitattu 13.12.2009]. Saatavissa: http://tools.ietf.org/html/rfc2661

Understanding wireless LAN bridges. 2003. Jim Geier [viitattu 13.12.2009]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/1563991

VPN Overview. 2003. Microsoft Corporation [viitattu 13.12.2009]. Saatavissa: http://download.microsoft.com/download/0/e/3/0e354109-5a05-48f2-a557-8c49f5230d8f/vpnoverview.doc

VPN-verkot. 2009. 2k mediat [viitattu 13.12.2009]. Saatavissa:

http://www.2kmediat.com/vpn/yhteys.asp

VPN. 2009. Viestintävirasto [viitattu 13.12.2009]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html

VTUN FAQ 2009. 2009. VTUN [viitattu 13.12.2009]. Saatavissa: http://vtun.sourceforge.net/faq.html

Virtualisointi. 2011. Isoworks [viitattu 12.2.2011] Saatavissa: http://www.isoworks.fi/fi/ratkaisumme/erillispalvelut/palvelinratkaisut/virtualisointi

Virtualization Basics. 2011. VMware, Inc. [viitattu 12.2.2011]. Saatavissa: http://www.vmware.com/virtualization/virtual-machine.html

Web Server (IIS) Role Overview. Microsoft Technet [viitattu 22.2.2011]. Saatavissa: http://technet.microsoft.com/en-us/library/cc770634.aspx

What is web server. 2011. Web developers notes. Wikipedia [viitattu 12.2.2011]. Saatavissa: http://www.webdevelopersnotes.com/basics/what_is_web_server.php

Wikipedia 2011a. Bind. Wikipedia [viitattu 12.2.2011]. Saatavissa: http://en.wikipedia.org/wiki/BIND

Wikipedia 2011b. Microsoft DNS. [viitattu 12.2.2011]. Saatavissa: http://en.wikipedia.org/wiki/Microsoft_DNS

Wikipedia 2011c. Apache HTTP Server. Wikipedia [viitattu 12.2.2011]. Saatavissa: http://en.wikipedia.org/wiki/Apache_HTTP_Server

LIITTEET

Liitteet on poistettu, koska niitä ei haluttu julkistaa.